IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An apparatus for generating pseudorandom sequences comprising:

a cellular automata random number generator of a first type ~~for generating~~ configured to generate a first sequence with ~~higher~~ a first predetermined randomness and a first predetermined period;

a cellular automata random number generator of a second type ~~for generating~~ configured to generate a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined ~~lower bound on the~~ period larger that the first predetermined period; and

adders ~~for performing~~ configured to perform bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 2 (Currently Amended): The apparatus according to claim 1, wherein:

the cellular automata random number generator of a first type is two-dimensional cellular automata;

the cellular automata random number generator of a second type is 2-by-L cellular automata; and

~~the~~ summation results from the adders are outputted as the pseudorandom sequences.

Claim 3 (Currently Amended): The apparatus according to claim 1, further comprising:

a cellular automata random number generator of a third type ~~for generating~~ configured to generate a third sequence, the cellular automata random number generator of a third type

~~having cells whose~~ determines cell states ~~can be computed~~ based on a corresponding cell control word and/or a corresponding rule control word; wherein

the cell control word is generated by the cellular automata random number generator of a second type;

the rule control word is generated by the cellular automata random number generator of a first type; and

the adders ~~for performing~~ perform bit-to-bit mod2 sum of the first, the second and the third sequences.

Claim 4 (Currently Amended): The apparatus according to claim 3, wherein:

the summation results from the adders are outputted as ~~the~~ pseudorandom sequences.

Claim 5 (Currently Amended): The apparatus according to claim 2 further comprising:

a first block ~~for performing~~ configured to perform a nonlinear mapping on the summation results from the adders; and

a second block ~~for~~ configured to perform a non-uniform decimation on the results of the nonlinear ~~mapping;~~ mapping, wherein the decimated result is outputted as the pseudorandom sequence.

Claim 6 (Previously Presented): The apparatus according to claim 5, wherein:

each of the blocks includes at least one nonlinear function.

Claim 7 (Currently Amended): The apparatus according to claim 5, wherein:

the second block ~~for performing nonlinear mapping~~ includes at least one look-up table for nonlinear mapping based on the Latin squares.

Claim 8 (Currently Amended): An apparatus for performing cryptographic processing ~~characterized by~~ comprising:

a cryptographic processor for encrypting data using pseudorandom sequences; and

a pseudorandom sequence generator for generating ~~the~~ pseudorandom ~~sequences;~~ sequences, wherein the pseudorandom number generator is configured to include the apparatus according to claim 1.

Claim 9 (Currently Amended): A method for generating pseudorandom sequences using cellular automata in a pseudorandom sequence generator comprising:

generating, at a cellular automata random number generator of a first type, a first sequence with ~~higher~~ a first predetermined randomness and a first predetermined period;

generating, at a cellular automata random number generator of a second type, a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined ~~lower bound on the~~ period larger that the first predetermined period; and

performing, at an adder, bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 10 (Canceled)

Claim 11 (Currently Amended): A computer readable recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the ~~recording medium wherein~~ the method comprising:

generating a first sequence with ~~higher~~ a first predetermined randomness and a first predetermined period;

generating a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined ~~lower bound on the~~ period larger that the first predetermined period; and

performing bit-to-bit mod2 sum of the first sequences and the second sequences.

Claim 12 (New): The apparatus according to claim 1, wherein the first sequence generated by the cellular automata random number generator of a first type satisfies the DIEHARD test.